EVALUATION REPORT

Independent Evaluation of NRC's
Implementation of the Federal
Information Security Management Act
(FISMA) for Fiscal Year 2005

OIG-05-A-21 September 30, 2005

September 30, 2005

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

FROM: Stephen D. Dingbaum/**RA**/
Assistant Inspector General for Audits

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) FOR FISCAL YEAR 2005 (OIG-05-A-21)

Attached please find the Office of the Inspector General's report, *Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2005*. This report reflects the results of the independent evaluation performed by Richard S. Carson & Associates, Inc., on behalf of the NRC Office of the Inspector General.

Basing this review on the Office of Management and Budget's criteria for FISMA compliance, Richard S. Carson & Associates, Inc., determined that the NRC's information security program has several weaknesses.

During an exit conference on September 22, 2005, NRC officials provided comments concerning the draft audit report and subsequently opted not to submit formal written comments to this report.

If you have any questions or wish to discuss this report, please call me at 415-5915 or Beth Serepca at 415-5911.

Attachment: As stated

Distribution

John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
G. Paul Bollwerk, III, Chief Administrative Judge, Atomic Safety andT Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Janice Dunn Lee, Director, Office of International Programs
William N. Outlaw, Director of Communications
William N. Outlaw, Acting Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
William F. Kane, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration, and Chief Information Officer, OEDO
William M. Dean, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Michael R. Johnson, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Carl J. Paperiello, Director, Office of Nuclear Regulatory Research
Paul H. Lohaus, Director, Office of State and Tribal Programs
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act For Fiscal Year 2005

Contract Number: GS-00F-0001N
Delivery Order Number: DR-36-03-346

September 30, 2005

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which includes an annual independent evaluation of the agency's information security program[1] and practices to determine their effectiveness. This evaluation must include testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems. FISMA requires the annual evaluation to be performed by the agency's Inspector General (IG) or by an independent external auditor.

Office of Management and Budget (OMB) memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated June 13, 2005, requires the agency's IG to complete the Reporting Template for Agency IGs. That template, along with any additional narrative the IG feels provides meaningful insight into the status of the agency's security or privacy program, is submitted to OMB as part of the agency's annual FISMA report.

Richard S. Carson and Associates, Inc., (Carson Associates) performed an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA for FY 2005. This report presents the results of that independent evaluation. Carson Associates also prepared the Reporting Template for Agency IGs, along with additional narrative, for inclusion in the agency's annual FISMA report. The Reporting Template for Agency IGs and the additional narrative is included as Appendix C to this report.

The OIG also asked Carson Associates to evaluate the agency's compliance with the Privacy Act. This request was made prior to OMB's issuance of the FY 2005 FISMA reporting guidelines, which also include a requirement to report on implementation of the Privacy Act.

PURPOSE

The objective of this review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2005.

[1] NRC uses the term information security program to describe its program for ensuring that various types of sensitive information are handled appropriately and are protected from unauthorized disclosure in accordance with pertinent laws, Executive orders, management directives, and applicable directives of other Federal agencies and organizations. For the purposes of FISMA, the agency uses the term automated information security program.

RESULTS IN BRIEF

While major deficiencies exist, NRC has made improvements to its automated information security program. For example:

- The agency has corrected 66 percent of its program level weaknesses and 7 percent of its system level weaknesses reported on its plans of action and milestones (POA&Ms).
- The agency developed templates for risk assessments, security plans, security test and evaluation plans, security test and evaluation reports, contingency plans, and contingency plan test reports. The templates and instructions for their use are available on the NRC information technology (IT) security Web page. The templates were developed to ensure security documentation supporting system certification and accreditation is consistent with guidelines from the National Institute of Standards and Technology (NIST). The templates include a section or sections that specifically identify action items resulting from the certification and accreditation process to ensure corrective actions are tracked.
- The agency requires that the system certification package contain a spreadsheet of the plan to resolve issues identified during the certification process. This requirement is also presented on the agency's IT security Web page.
- The agency modified the security plan template and the NRC version of the self-assessment based on NIST Special Publication (SP) 800-26, *Self-Assessment Guide for Information Technology Systems*, to ensure security protection requirements (confidentiality, integrity, and availability) are consistently defined.

However, the independent evaluation identified the following automated information security program weaknesses.

- The majority of NRC systems have not been categorized in accordance with Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.*
- Agency self-assessments are not timely.
- Annual contingency plan testing is not being performed.
- The agency does not maintain documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements.
- Oversight of other contractor systems is lacking.
- The agency's inventory of information systems is only 51-70 percent complete because (1) information in the two systems that maintain inventory information is inaccurate and inconsistent and (2) only one system contains information on system interfaces and that information is also inaccurate and inconsistent. In addition, the agency's inventory is not maintained and updated annually.

- E-authentication risk assessments completed in accordance with OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, are incorrect and inconsistent with the systems' FIPS 199 security categorizations.
- The agency is not always following OMB's POA&M guidance and the metrics submitted to OMB deviate from the actual POA&Ms.
- The majority of the agency's operational information systems (19 of 27) are operating under an interim authorization to operate (IATO), and therefore are not considered certified and accredited.
- The agency lacks procedures for ensuring employees with significant IT security responsibilities receive security training and awareness.

RECOMMENDATIONS

This report makes recommendations to the Executive Director for Operations to improve NRC's automated information security program and implementation of FISMA. A consolidated list of recommendations appears on page 25 of this report.

AGENCY COMMENTS

The OIG provided this report in draft to agency officials and discussed its content at an exit conference on September 22, 2005. We modified the report as we determined appropriate in response to our discussion. Agency officials generally agreed with the report's findings and recommendations and opted not to include formal comments.

[Page intentionally left blank]

ABBREVIATIONS AND ACRONYMS

ADAMS	Agencywide Document Access and Management System
AIS	Automated Information System
Carson Associates	Richard S. Carson and Associates, Inc.
CFR	Code of Federal Regulations
CIO	Chief Information Officer
Data Center	Data Center/Telecommunications System
DDMS	Digital Data Management System
EARS	Enterprise Architecture Repository System
EHD	Electronic Hearing Docket
EIE	Electronic Information Exchange
ERDS	Emergency Response Data System
ETS	Emergency Telecommunications System
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GLTS	General License Tracking System
HLW EHD	High Level Waste Electronic Hearing Docket
HPCS	High Performance Computing System
IATO	Interim Authorization to Operate
IG	Inspector General
IPSS	Integrated Personnel Security System
IT	Information Technology
ITSSTS	Information Technology Systems Security Tracking System
LAN/WAN	Local Area Network/Wide Area Network
LSN	Licensing Support Network
LTS	License Tracking System
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCIMS	Operations Center Information Management System

OIG	Office of the Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget
OPM	Office of Personnel Management
POA&M	Plan of Action and Milestones
RPS	Reactor Program System
SP	Special Publication
SQL	Structured Query Language
TAC	Technology Assessment Center
US-CERT	United States Computer Emergency Readiness Team
U.S.C.	United States Code

TABLE OF CONTENTS

[Page intentionally left blank]

1 Background

On December 17, 2002, the President signed the E-Government Act of 2002, which included FISMA.[2] FISMA outlines the information security management requirements for agencies, which includes an annual independent evaluation of the agency's information security program and practices to determine their effectiveness. This evaluation must include testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems. FISMA requires the annual evaluation to be performed by the agency's IG or by an independent external auditor.

OMB memorandum M-05-15 requires the agency's IG to complete the Reporting Template for Agency IGs. That template, along with any additional narrative the IG feels provides meaningful insight into the status of the agency's security or privacy program, is submitted to OMB as part of the agency's annual FISMA report.

Carson Associates performed an independent evaluation of NRC's implementation of FISMA for FY 2005. This report presents the results of that independent evaluation. Carson Associates also prepared the Reporting Template for Agency IGs, along with additional narrative, for inclusion in the agency's annual FISMA report. The Reporting Template for Agency IGs and the additional narrative is included as Appendix C to this report.

The OIG also asked Carson Associates to evaluate the agency's compliance with the Privacy Act.[3] This request was made prior to OMB's issuance of the FY 2005 FISMA reporting guidelines, which also include a requirement to report on implementation of the Privacy Act.

2 Purpose

The objective of this review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2005.

3 Findings

While major deficiencies exist, NRC has made improvements to its automated information security program.

- The agency has corrected 66 percent of its program level weaknesses and 7 percent of its system level weaknesses reported on its POA&Ms.

[2] The Federal Information Security Management Act of 2002 was enacted on December 17, 2002, as part of the E-Government Act of 2002 (Public Law 107-347), and replaces the Government Information Security Reform Act, which expired in November 2002.

[3] The Privacy Act of 1974 (5 U.S.C. § 552a), As Amended, was enacted to balance the Government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy resulting from the collection, maintenance, use, and disclosure of personal information. The Privacy Act safeguards confidentiality by limiting or restricting disclosure of personally identifiable records maintained by Federal agencies.

- The agency developed templates for risk assessments, security plans, security test and evaluation plans, security test and evaluation reports, contingency plans, and contingency plan test reports. The templates and instructions for their use are available on the NRC IT security Web page. The templates were developed to ensure security documentation supporting system certification and accreditation is consistent with guidelines from NIST. The templates include a section or sections that specifically identify action items resulting from the certification and accreditation process to ensure corrective actions are tracked.
- The agency requires that the system certification package contain a spreadsheet of the plan to resolve issues identified during the certification process. This requirement is also presented on the agency's IT security Web page.
- The agency modified the security plan template and the NRC version of the self-assessment based on NIST SP 800-26 to ensure security protection requirements (confidentiality, integrity, and availability) are consistently defined.

However, the independent evaluation identified the following automated information security program weaknesses.

- The majority of NRC systems have not been categorized in accordance with FIPS 199.
- Agency self-assessments are not timely.
- Annual contingency plan testing is not being performed.
- The agency does not maintain documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements.
- Oversight of other contractor systems is lacking.
- The agency's inventory of information systems is only 51-70 percent complete because (1) information in the two systems that maintain inventory information is inaccurate and inconsistent and (2) only one system contains information on system interfaces and that information is also inaccurate and inconsistent. In addition, the agency's inventory is not maintained and updated annually.
- E-authentication risk assessments completed in accordance with OMB M-04-04 are incorrect and inconsistent with the systems' FIPS 199 security categorizations.
- The agency is not always following OMB's POA&M guidance and the metrics submitted to OMB deviate from the actual POA&Ms.
- The majority of the agency's operational information systems (19 of 27) are operating under an IATO, and therefore are not considered certified and accredited.
- The agency lacks procedures for ensuring employees with significant IT security responsibilities receive security training and awareness.

The following sections present the detailed findings from the independent evaluation. The format of the following sections is based on the FY 2005 FISMA Reporting Template for Agency IGs, which can be found in Appendix C.

3.1 Agency and Contractor Systems

Agency Systems

FY 2005 FISMA Reporting Template for Inspectors General Question 1.a

Table 3-1. FY 05 Agency Systems

FIPS 199 Risk Impact Level	Total Number	Number Reviewed
High	4	0
Moderate	4	0
Low	0	0
Not Categorized	19	0
Total	27	0

NRC has a total of 30 production systems. Of the 30, 12 are general support systems[4] (all operational), and 18 are major applications[5] (15 operational, 3 in development). As required by FISMA, the NRC Office of the Inspector General (OIG) selected five NRC operational systems for evaluation during the FY 2005 FISMA independent evaluation. However, during a status meeting with the agency, the OIG learned that the certification and accreditations of the systems chosen for evaluation had either expired and the systems are operating under an IATO, or were due to expire in FY 2005, and that their re-certification and re-accreditation would not be completed before completion of the FY 2005 FISMA independent evaluation. Furthermore, there were no other systems to substitute because they were either reviewed during the FY 2004 FISMA independent evaluation, or had certification and accreditations that were due to expire before the end of the year. Without enough systems with current certification and accreditations, Carson Associates could not perform an evaluation of a representative subset of agency systems for the FY 2005 FISMA independent evaluation.

Contractor Systems

FY 2005 FISMA Reporting Template for Inspectors General Question 1.b

Table 3-2. FY 05 Contractor Systems

FIPS 199 Risk Impact Level	Total Number	Number Reviewed
High	0	0
Moderate	0	0
Low	0	0
Not Categorized	7	0
Total	7	0

[4] A general support system is an interconnected set of information resources under the same direct management control that share common functionality. Typical general support systems are local and wide area networks, servers, and data processing centers.

[5] A major application is a computerized information system or application that requires special attention to security because of the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of the information in the application.

NRC has a total of seven systems operated by a contractor or other organization on behalf of the agency (two major applications and five general support systems). Of the seven, three are operated by other Federal agencies, two are operated by federally funded research and development centers, and two are operated by contractors supporting the agency. The OIG did not review any of the seven systems operated by a contractor or other organization on behalf of the agency for evaluation during the FY 2005 FISMA independent evaluation, as there were no potential candidates to review. Of the seven, four[6] were evaluated during the FY 2004 FISMA independent evaluation (three operated by other Federal agencies and one operated by a federally funded research and development center), and therefore were not candidates for review in FY 2005. The other three systems operated by a contractor or other organization on behalf of the agency were not candidates for evaluation in FY 2005 because there was not sufficient information available to perform an evaluation. The agency stated that in FY 2005 it would be performing self-assessments in accordance with NIST SP 800-26 on its contractor systems. However, the self-assessments were not completed in time for inclusion in the FY 2005 FISMA independent evaluation.

Majority of NRC Systems Have Not Been Categorized in Accordance With FIPS 199

FIPS 199 requires all agencies to categorize their information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. All systems must be categorized using FIPS 199 by February 2005.

However, despite the requirement to categorize all systems by February 2005, Carson Associates found that the majority of NRC information systems, including systems operated by a contractor or other organization on behalf of the agency, have not been categorized in accordance with FIPS 199. Specifically, only 8 of the 27 operational NRC information systems have been categorized and none of the contractor systems have been categorized.

Not only is security categorization required by FIPS 199, it is needed to select the minimum security controls for a system as defined in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. As a result, the agency cannot determine the appropriate minimum security controls for its information systems and cannot determine whether the current controls for the information systems are adequate.

[6] The FY 2004 FISMA independent evaluation included a review of three contractor operations and facilities. These three contractor operations and facilities support a total of four agency systems operated by a contractor or other organization on the behalf of the agency.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Categorize all NRC information systems, including systems operated by a contractor or other organization on behalf of the agency, in accordance with FIPS 199.

3.2 Agency Performance of FISMA Activities

3.2.1 Certification and Accreditation

FY 2005 FISMA Reporting Template for Inspectors General Question 2.a

Table 3-3. Number of Systems Certified and Accredited

FIPS 199 Risk Impact Level	Agency	Contractor	Total
High	1	0	1
Moderate	0	0	0
Low	0	0	0
Not Categorized	7	3	10
Total	8	3	11

Agency Systems

As stated previously, during a status meeting with the agency the OIG learned that the certification and accreditations of some agency information systems had either expired and the systems are operating under an IATO, or were due to expire in FY 2005. Specifically, only 8 of the 27 operational NRC information systems have full authorization to operate (i.e., they have a current certification and accreditation). The lack of systems with current certification and accreditations prompted OIG to request Carson Associates to undertake an overall review of the NRC's certification and accreditation efforts. Section 3.7 of this report discusses the OIG's assessment of the agency's certification and accreditation process in detail.

Contractor Systems

Of the seven systems operated by a contractor or other organization on behalf of the agency, only three have been certified and accredited. These three systems are operated by other Federal agencies. NRC presumes that the two Federal agencies that operate these systems are also following FISMA and NIST guidelines (these agencies have not allowed NRC to conduct their own review). Carson Associates verified that there are agreements in place with the two Federal agencies providing services to NRC and that the agreements include requirements to comply with applicable Federal and respective agency information systems security policies, mandates, and instructions. However, the agency does not maintain copies of all certification and accreditation documentation for these systems. The other four systems operated by a contractor or other organization on behalf of the agency have not been certified and accredited.

3.2.2 Security Control Test and Evaluation

FY 2005 FISMA Reporting Template for Inspectors General Question 2.b

Table 3-4. Number of Systems With Tested and Evaluated Security Controls

FIPS 199 Risk Impact Level	Agency	Contractor	Total
High	2	0	2
Moderate	2	0	2
Low	0	0	0
Not Categorized	14	3	17
Total	18	3	21

Agency Systems

FISMA requires agencies to test and evaluate the security controls of every information system identified in their inventory no less than annually. The necessary depth and breadth of an annual FISMA review depends on several factors such as (1) the potential risk and magnitude of harm to the system or data, (2) the relative comprehensiveness of last year's review, and (3) the adequacy and successful implementation of the POA&M for weaknesses in the system. For example, if last year a system underwent a complete certification and accreditation, this year a relatively simple update or maintenance review using NIST's self-assessment guidance may be sufficient, provided it has been adequately documented within the agency. Previous OMB FISMA guidance stated agencies must use NIST SP 800-26 to conduct their annual reviews. The FY 2005 FISMA guidance allows agencies to continue to use NIST SP 800-26, or to conduct a self-assessment against the controls found in NIST SP 800-53.

NRC meets the FISMA requirement to test and evaluate the security controls of agency information system by performing annual self-assessments on the systems. As in previous years, NRC developed self-assessment templates for major applications and general support systems. For FY 2005 NRC also developed a site self-assessment template for security assessments at regional offices, resident inspector sites, NRC locations other than headquarters and the regional offices, and contractor sites hosting NRC information systems. The NRC self-assessment templates are based on NIST SP 800-26 and include references to NIST SP 800-53 to provide a general indication of control coverage. While the templates include references to NIST SP 800-53, the intent is not to perform a self-assessment against the controls found in NIST SP 800-53, but rather to provide organizations with a general indication of control coverage.

As of September 12, 2005, Carson Associates has only received self-assessments for 18 of NRC's 27 operational information systems.[7] The first self-assessment was not received until September 2, 2005. Subsequent to completion of field work, the agency provided self-assessments for the other nine operational systems. However, these self-assessments were not provided in time to review.

[7] One of the self-assessments addresses eight individual general support systems.

Contractor Systems

Of the seven systems operated by a contractor or other organization on behalf of the agency, only three have had their security controls tested and evaluated in the last year. These three systems are operated by other Federal agencies. NRC presumes that the two Federal agencies that operate these systems are also following FISMA and NIST guidelines (these agencies have not allowed NRC to conduct their own review), and have therefore conducted an annual review. However, the agency does not request a copy of the annual review for these systems from the other Federal agencies.

As previously discussed, the agency stated that in FY 2005 it would be performing self-assessments on its contractor systems. However, Carson Associates has not received any self-assessments for the four other systems operated by a contractor or other organization on behalf of the agency. Subsequent to completion of field work, the agency provided self-assessments for the four other systems operated by a contractor or other organization on behalf of the agency. However, these self-assessments were not provided in time to review.

Agency Self-Assessments Are Not Timely

As stated previously, NRC meets the requirement for annual test and evaluation of security controls for agency information systems by conducting self-assessments. The agency includes self-assessment activities in its POA&Ms. The majority of self-assessments were scheduled for completion by August 1, 2005, according to the 3rd Quarter FY 2005 POA&Ms submitted to OMB. The agency also stated that it would be conducting self-assessments on regional offices, resident inspector sites, NRC locations other than headquarters and the regional offices, and contractor sites hosting NRC information systems.

However, despite the requirement to perform annual test and evaluation of security controls for agency information systems, and despite the agency's commitment to complete self-assessments by August 1, 2005, Carson Associates found that self-assessments have been completed for only 18 of the agency's 27 operational information systems (as of September 12, 2005). As a result, the agency is not meeting FISMA requirements for performing annual test and evaluation of security controls.

Lack of self-assessments also impacts the completeness of the OIG's independent evaluation of the agency's implementation of FISMA. As required by FISMA, the OIG selects a subset of agency information systems for evaluation. In addition to the detailed review of the subset of agency information systems, the OIG also performs a high level review of all agency information systems by reviewing their current self-assessments. However, for the FY 2005 FISMA independent evaluation, the agency did not provide the OIG with the self-assessments in time to perform the high level review.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

2. Complete annual self-assessments for FY 2006 no later than August 1, 2006, and thereafter.

3.2.3 Contingency Planning and Testing

FY 2005 FISMA Reporting Template for Inspectors General Question 2.c

Table 3-5. Number of Systems With Tested Contingency Plans

FIPS 199 Risk Impact Level	Agency	Contractor	Total
High	0	0	0
Moderate	1	0	1
Low	0	0	0
Not Categorized	2	3	5
Total	3	3	6

Agency Systems

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, states that contingency plans should be tested at least annually and when significant changes are made to the information system, supported business process(s), or the contingency plan. As of September 12, 2005, Carson Associates has only received results of contingency plan testing for 3 of NRC's 27 operational information systems. Subsequent to the completion of field work, Carson Associates was informed that contingency plan testing had been performed on 10 additional agency systems (8 of which are general support systems resulting from the decomposition of the agency's local area network/wide area network general support system). However, the agency has not provided documentation indicating the testing has been completed.

Contractor Systems

Of the seven systems operated by a contractor or other organization on behalf of the agency, only three have had their contingency plans tested in the last year. These three systems are operated by other Federal agencies. NRC presumes that the two Federal agencies that operate these systems are also following FISMA and NIST guidelines (these agencies have not allowed NRC to conduct their own review), and have therefore performed an annual contingency plan test of their systems. However, the agency does not verify that the contingency plans have been tested and evaluated for these systems on an annual basis. The agency does not have contingency plans for the other four systems operated by a contractor or other organization on behalf of the agency.

Annual Contingency Plan Testing Is Not Being Performed

As stated previously, NIST SP 800-34 states that contingency plans should be tested at least annually. However, despite this requirement, Carson Associates found that only 3 of the agency's 27 operational information systems have had their contingency plans tested in FY 2005.

The 3rd Quarter FY 2005 POA&Ms the agency submitted to OMB included information on the status of contingency plan testing for the agency's 24 operational information systems that have not yet had their contingency plans tested. According to the 3rd Quarter FY 2005 POA&Ms, the delays in testing the contingency plans are related to the delays in certifying and accrediting the systems. The following is a summary of the reasons for the delays for the 24 systems that have not had their contingency plans tested in FY 2005. See Appendix B for additional details on the status of contingency plan testing.

- Of the 24, 18 are undergoing re-certification and re-accreditation (6 of the 18 have a current certification and accreditation and the other 12 have an expired certification and accreditation and are operating under an IATO).
- Of the 24, 4 are undergoing certification and accreditation for the first time.
- Of the 24, 1 is scheduled to be transitioned to a research and development role by December 31, 2005, and would no longer require certification and accreditation.
- Of the 24, 1 was not included with the 3rd Quarter FY 2005 POA&Ms, but this system is new, and is undergoing certification and accreditation for the first time.

The testing of contingency plans is essential in determining whether plans will function as intended in an emergency situation. Without testing, the agency has limited assurance that it will be able to recover mission-critical applications, business processes, and information in the event of an unexpected interruption. Even a minor interruption could result in lost or incorrectly processed data if the contingency plan has not been tested.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

3. Develop and implement procedures to ensure contingency plans are tested annually, regardless of the status of the systems' certification and accreditation.

3.3 Agency Oversight

FY 2005 FISMA Reporting Template for Inspectors General Question 3.a

3.a. The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient.	*Mostly, for example, approximately 81-95% of the time*

FISMA requires agencies to provide information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (1) information collected or maintained by or on behalf of the agency and (2) information systems used or operated by an agency or other organization on behalf of an agency.[8] OMB M-05-15 provides examples of agency security responsibilities concerning contractors and other sources. OMB M-05-15 describes the following primary categories of contractors as they relate to securing systems and information.

- **Service providers** – encompasses typical outsourcing of system or network operations, telecommunications services, or other managed services. OMB states that agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not "equivalent," security procedures. For example, annual reviews, risk assessments, security plans, control testing, contingency planning, and certification and accreditation must, at a minimum, explicitly meet guidance from NIST. NRC has three contractor systems that fit in this category. All three of these systems are operated by other Federal agencies.
- **Contractor support** – encompasses on or offsite contractor technical or other support staff. As with service providers, OMB states that agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not "equivalent," security procedures. Specifically, the agency is responsible for ensuring the contractor personnel receive appropriate training (i.e., general and specific). NRC has two contractor systems that fit in this category.
- **Government-owned, contractor-operated facilities** – includes federally funded research and development centers. OMB states that these facilities are agency components and their security requirements are identical to those of the managing Federal agency in all respects. Security requirements must be included in the terms of the contract. NRC has two contractor systems that fit in this category. The managing Federal agency for one of the systems is NRC and the other is another Federal agency.

[8] Information systems used or operated by a contractor of an agency or other organization on behalf of the agency refers to information systems that the agency considers to be either major applications or general support systems.

Agency Does Not Maintain Documentation That Demonstrates Systems Provided By Other Federal Agencies Meet FISMA Requirements

NRC presumes that the two Federal agencies that operate three of the seven contractor systems are also following FISMA and NIST guidelines (these agencies have not allowed NRC to conduct their own review). Carson Associates verified that there are agreements in place with the two Federal agencies providing services to NRC and that the agreements include requirements to comply with applicable Federal and respective agency information systems security policies, mandates, and instructions. Carson Associates also verified that the agency has copies of current security plans for two of the three systems. However, the agency does not (1) maintain copies of all certification and accreditation documentation for these systems, (2) verify that the security controls have been tested and evaluated for these systems on an annual basis, and (3) verify that the contingency plans have been tested and evaluated for these systems on an annual basis.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

4. Maintain current copies of certification and accreditation memoranda for systems provided by other Federal agencies.
5. Maintain current copies of self-assessments for systems provided by other Federal agencies.
6. Maintain current copies of annual contingency plan testing results for systems provided by other Federal agencies.

Oversight of Other Contractor Systems Is Lacking

The agency has not performed sufficient oversight and evaluation of four of the seven contractor systems to ensure the information systems meet requirements of FISMA, OMB policy, NIST guidelines, and agency policy. The agency stated that for two of the four systems (the two contractor support systems), security guidelines are written into the relevant contracts and the contractors must follow NRC security procedures. However, the agency has no documentation demonstrating that these systems meet FISMA requirements, specifically the requirement for certification and accreditation, annual testing and evaluation of security controls, and annual contingency plan testing. Carson Associates could not determine how NRC performs oversight of the other two contractor systems (the two federally funded research and development centers).

Oversight of other contractor systems is lacking because the agency lacks procedures for performing this oversight. For example, Management Directive (MD) and Handbook 12.5, *NRC Automated Information Security Program*, require all NRC major applications and general support systems to be certified and accredited, and describes the procedures for accomplishing certification and accreditation. However, MD and Handbook 12.5 do not describe procedures for certifying and accrediting major applications and general support systems operated by a contractor or other organization on behalf of the agency.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

7. Develop and implement procedures for performing oversight of major applications and general support systems operated by a contractor or other organization on behalf of the agency.

3.4 Agency System Inventory

FY 2005 FISMA Reporting Template for Inspectors General Questions 3.b, 3.c, 3.d, 3.e

3.b. The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.	*Approximately 51-70% complete*
*3.c. The OIG **generally** agrees with the CIO on the number of agency owned systems.*	*No*
*3.d. The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.*	*Yes*
3.e. The agency inventory is maintained and updated at least annually.	*No*

FISMA requires agencies to develop and maintain an inventory of major information systems operated by or under control of the agency. The inventory must include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency, and must be updated at least annually. The inventory shall also be used to support information resources management.

MD and Handbook 12.5 assign the NRC Chief Information Officer (CIO) responsibility for developing and maintaining a master inventory of all agency systems. MD and Handbook 2.1, *Information Technology Architecture*, assign the NRC CIO responsibility for developing, maintaining, and implementing the NRC Information Technology Architecture. The agency maintains two inventories, the Information Technology Systems Security Tracking System (ITSSTS) and the Enterprise Architecture Repository System (EARS), to meet the requirements outlined in MD and Handbooks 12.5 and 2.1, respectively.

While FISMA only requires agencies to maintain an inventory of major information systems (major applications and general support systems), NRC also includes two other types of systems in its inventories.

- **Listed** – a computerized information system or application that (1) processes sensitive information requiring additional security protections and (2) may be important to an NRC

office's or region's operations, but which is not a major application or general support system when viewed from an agency perspective. Sensitive data may include individual Privacy Act information, law enforcement sensitive information, sensitive contractual and financial information, safeguards, and classified information.

- **Other** – an NRC system that does not require additional security protections and is adequately protected by the security provided by the NRC local area network/wide area network.

Carson Associates found that the agency's inventory is only 51-70 percent completed because (1) information in both ITSSTS and EARS is inaccurate and inconsistent and (2) only EARS contains information on system interfaces and that information is also inaccurate and inconsistent. Carson Associates generally agrees with the CIO on the number of agency owned major applications and general support systems, but does not agree with the CIO on the number of agency owned systems in the listed and other categories. Carson Associates also found that the agency's inventory is not maintained and updated at least annually.

As requested by the OIG, Carson Associates conducted a separate evaluation of the agency's automated information system (AIS) inventory process. The findings from this review were reported separately under OIG-05-A-22, *Office of the Inspector General Evaluation of NRC's Automated Information System Inventory Process*. The report made seven recommendations to the agency to improve its inventory process. The following is a summary of the findings from the evaluation of NRC's AIS inventory process.

The evaluation of the agency's AIS inventory process found that (1) information in NRC AIS inventories is inaccurate and inconsistent and (2) NRC AIS inventory systems are not designed to capture all of the data needed to meet FISMA requirements. The information in NRC AIS inventories is inaccurate and inconsistent because the procedures for maintaining and updating AIS inventories are inadequate. Specifically, the agency (1) lacks procedures for updating AIS inventories with information collected from office directors, regional administrators, and system sponsors/owners, (2) provides insufficient guidance to office directors, regional administrators, and system sponsors/owners when requesting information for the AIS inventories, (3) lacks procedures for adding new systems to the AIS inventories, and (4) lacks procedures for updating information for systems already in the inventory. The lack of adequate procedures not only results in the inaccurate and inconsistent data, but also results in duplicative efforts for NRC offices.

As a result of inaccurate and inconsistent data in the AIS inventories, the agency lacks a complete understanding of what AISs are currently in use, and therefore cannot support two of the five areas of information resources management specified by FISMA. Without an accurate AIS inventory, the agency cannot adequately plan, budget, acquire, and manage information technology without first knowing what information technology is currently in place. The agency also cannot adequately monitor, test, and evaluate security controls for AIS as required by FISMA.

Neither ITSSTS nor EARS were designed to capture all of the data needed to fully meet FISMA's requirement to develop an inventory of major information systems that shall be used to

support information resources management. For example, only one inventory system captures the data needed to indicate which systems include Privacy Act data, and not all systems that include Privacy Act data are correctly identified. Therefore the agency cannot provide effective privacy protections, and cannot test and evaluate those protections, if it cannot identify which systems contain Privacy Act data. In addition, neither inventory system captures the data needed to support (1) preparation and maintenance of the inventory of information resources required to support the Government Information Locator Service, (2) preparation of the index of major information systems required under the Freedom of Information Act, and (3) preparation of information system inventories required for records management.

3.5 E-Authentication

FY 2005 FISMA Reporting Template for Inspectors General Questions 3.f

3.f. The agency has completed system e-authentication risk assessments.	*No*

In FY 2004, the agency stated that it had begun assessing systems for e-authentication risk in accordance with OMB M-04-04. A contract was awarded in the 3rd Quarter FY 2004 and the agency stated that it was on track to meet the December 15, 2004, deadline for classifying all major applications. OMB M-04-04 required all systems classified as "major" to implement the guidance by December 15, 2004, and the remaining systems to implement the guidance by September 15, 2005. New systems are required to implement the guidance within 90 days of the completion of the final e-authentication technical guidance issued by NIST (NIST issued the final guidance in June 2004).

E-Authentications Are Incorrect and Inconsistent

Despite these requirements, and the agency's previous statement that it was on track to meet the December 15, 2004, deadline for classifying all major applications, Carson Associates found that e-authentication risk assessments have been completed for only 6 of the agency's 27 operational systems. The agency stated that e-authentication risk assessments will be supported under the interim Information Systems Security contract awarded August 11, 2005, and are expected to be completed by December 15, 2005. Carson Associates reviewed the completed e-authentication risk assessments and found them to be incorrect and inconsistent with the systems' FIPS 199 security categorizations. For example, in some instances, the e-authentication assurance level was incorrectly determined based on the impact levels assigned to the six categories of harm and impact defined in OMB M-04-04. In other instances, the impact levels assigned to the six categories of harm and impact are not consistent with the FIPS 199 security categorizations of the systems.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

8. Review and update the six completed e-authentication risk assessments to correct inaccuracies and inconsistencies with FIPS 199 security categorizations.

9. Develop and implement a plan for completing the remaining e-authentication risk assessments.

3.6 Assessment of the POA&M Process

FY 2005 FISMA Reporting Template for Inspectors General Question 4

4.a. The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	*Almost Always, for example, approximately 96-100% of the time*
4.b. When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	*Almost Always, for example, approximately 96-100% of the time*
4.c. Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	*Almost Always, for example, approximately 96-100% of the time*
4.d. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	*Almost Always, for example, approximately 96-100% of the time*
4.e. OIG findings are incorporated into the POA&M process.	*Almost Always, for example, approximately 96-100% of the time*
4.f. POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	*Almost Always, for example, approximately 96-100% of the time*

NRC has two primary tools for tracking IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency. At a high level, NRC uses the POA&Ms submitted to OMB to track corrective actions from the OIG annual independent evaluation and the agency's annual review. The POA&Ms may also include corrective actions resulting from other security studies conducted by or on behalf of NRC.

At a more detailed level, NRC uses the ITSSTS to track the progress of more specific corrective actions, such as those resulting from risk assessments, security test and evaluation associated with the certification and accreditation process, and contingency plan testing.

The FY 2004 FISMA independent evaluation found that the agency's corrective action tracking process needed further improvement. Specifically, findings and recommendations resulting from security reviews and testing are not consistently being tracked and the agency's POA&M needed improvement. To address these weaknesses, the agency performed the following corrective actions.

- The agency developed templates for risk assessments, security plans, security test and evaluation reports, and contingency plan test reports that include a section or sections that

specifically identify action items resulting from the certification and accreditation process that should be tracked in ITSSTS. The templates and instructions for their use are available on the NRC IT security Web page. The agency also requires that the system certification package contain a spreadsheet of the plan to resolve issues identified during the certification process. This requirement is also presented on the IT security Web page.

- The agency reports corrected weaknesses on the POA&Ms for a year after their completion.
- The agency includes a completion date in the Status column of the POA&Ms.

In addition to improving its corrective action tracking progress, the agency has also made some progress in correcting weaknesses reported on its POA&Ms. The agency has corrected 66 percent of its program level weaknesses; however the agency has corrected only 7 percent of its system level weaknesses. The majority of delays have been caused by delays in completing certifications and accreditations, as described later in this report in Section 3.7.

In assessing the agency's POA&M process, Carson Associates also found that the agency is not always following OMB's POA&M guidance and that the metrics submitted to OMB often deviated from the actual POA&Ms.

NRC Has Made Some Progress in Correcting Weaknesses Reported on Its POA&Ms

The agency carried over a total of 2 program level and 12 system level weaknesses from FY 2004 into FY 2005. The following tables provide statistics from the three FY 2005 POA&Ms the agency has submitted to OMB.

Table 3-6. Program Level POA&Ms Statistics

Quarter	# At Start of Quarter	# New	# Completed	# On-going	# Delayed	# For Start of Next Quarter
Q1	2	10	3	7	2	9
Q2	9	0	3	4	2	6
Q3	6	0	2	2	2	4

Table 3-7. System Level POA&Ms Statistics

Quarter	# At Start of Quarter	# New	# Completed	# On-going	# Delayed	# For Start of Next Quarter
Q1	12	78	5	80	5	85
Q2	85	38	1	82	40	122
Q3	122	10	3	51	78	129

The following table summarizes the total number of weaknesses included in the FY 2005 POA&Ms, the total number of corrective actions the agency has reported as completed, the total number of corrective actions that are still on-going, and the number of corrective actions whose completion has been delayed.

Table 3-8. Summary of FY 2005 POA&Ms Through the 3rd Quarter

	Total # Weaknesses	Total # Completed	Total # On-going	Total # Delayed	% Completed
Program Level	12	8	2	2	66%
System Level	138	9	51	78	7%

The Agency Is Not Always Following OMB's POA&M Guidance

As stated previously, the agency is not always following OMB's POA&M guidance. The following are some examples of deviations from OMB's POA&M guidance found on the 2nd Quarter FY 2005 POA&Ms.

- A system level weakness was completely changed from the previous quarter. Data in the Weakness, Scheduled Completion Date, and Milestones with Completion Dates columns was changed. OMB guidance states that these columns should not be modified.
- Eight weaknesses had changes in the Scheduled Completion Date column. This column should not be modified.
- A system level weakness had comments added to the Milestones with Completion Dates column. This column should not be modified.
- Five system level weaknesses had minor modifications to dates in the Milestones with Completion Dates column. For example, a date in the format "May 2005" was modified to include the day of the week (e.g., 1-May-05). While this column should not be modified, the changes did not result in a change in a completion date.
- Two system level weaknesses had modifications to dates in the Milestones with Completion Dates column to correct typographical errors identified in a previous quarter (the year was incorrect in the previous quarter). The dates were also modified to include the day of the week. While this column should not be modified, the changes were to correct a typographical error. However, in both cases, one milestone date was also modified.
- One system level weakness had a milestone date in the 1st Quarter FY 2005 POA&Ms of 31-Jan-05. On the 2nd Quarter FY 2005 POA&Ms, the date was 08-Dec-04, which is a date that has already passed. Milestone dates for ongoing or delayed tasks should not be modified to a date that has already passed.

Carson Associates also found similar deviations from OMB's POA&M guidance on the 3rd Quarter FY 2005 POA&Ms. While the agency is not always following OMB's POA&M guidance, the agency is using the POA&Ms to track all known security weaknesses. Program officials report to the CIO on a quarterly basis on their remediation process. In some cases, program officials are required to report to the CIO on a monthly basis.

Metrics Submitted to OMB Deviate from the Actual POA&Ms

In addition to the deviations from OMB's POA&M guidance, Carson Associates also found discrepancies between the metrics submitted to OMB and the actual POA&Ms. However, the

discrepancies in the metrics are not significant enough to report as a weakness and are due, in part, to the large number of weaknesses being tracked on the agency's POA&Ms.

3.7 Assessment of the Certification and Accreditation Process

FY 2005 FISMA Reporting Template for Inspectors General Question 5

5. Assess the overall quality of the Department's certification and accreditation process.	*Poor*

The FY 2004 FISMA independent evaluation found that the agency's certification and accreditation process needed improvement. Specifically, the agency needed to develop processes for (1) ensuring security documentation supporting system certification and accreditation is consistent with NIST guidelines, (2) ensuring security protection requirements (confidentiality, integrity, availability) are consistently defined in security plans and self-assessments, and (3) ensuring security test and evaluation in support of certification and accreditation is comprehensive and independent. To address these weaknesses, the agency performed the following corrective actions.

- The agency developed templates for risk assessments, security plans, security test and evaluation plans, security test and evaluation reports, contingency plans, and contingency plan test reports. The templates and instructions for their use are available on the NRC IT security Web page. The templates were developed to ensure security documentation supporting system certification and accreditation is consistent with NIST guidelines.
- The agency modified the security plan template and the NRC version of the NIST SP 800-26 self-assessment to ensure security protection requirements (confidentiality, integrity, and availability) are consistently defined.
- The agency developed standard templates and instructions on their use for the security test and evaluation process. The templates and instructions are available on the NRC IT security Web page. The templates were developed to ensure security test and evaluation in support of certification and accreditation is comprehensive and independent.

Despite the improvements in the agency's certification and accreditation process, Carson Associates found that the majority of the agency's operational information systems operating under an IATO and therefore are not considered certified and accredited. As stated previously, only 8 of the 27 operational NRC information systems have full authorization to operate (i.e., they have a current certification and accreditation). As a result, the OIG requested Carson Associates to undertake an overall review of the NRC's certification and accreditation efforts. The findings from this review were reported separately under OIG-05-A-20, *Office of the Inspector General Evaluation of NRC's Certification and Accreditation Efforts*. The report made two recommendations to the agency to improve certification and accreditation efforts. The following is a summary of the findings from the evaluation of NRC's certification and accreditation efforts.

NRC's general support systems have not had a complete certification and accreditation performed in the past 3 years. Therefore the agency does not know whether the security controls for these general support systems are adequate, creating unknown potential risk. As a result, all NRC information systems that depend on the security controls provided by these general support systems inherit that unknown potential risk. The majority of NRC information systems are not certified and accredited because (1) the certification and accreditation has lapsed or was never completed and (2) NRC information systems are being re-certified and re-accredited using new NIST requirements.[9] As a result, potential risks to agency information systems are unknown.

3.8 Agency Security Configuration Policy

FY 2005 FISMA Reporting Template for Inspectors General Questions 6.a, 6.b

6.a. Is there an agency wide security configuration policy?	*Yes*
6.b. Are configuration guides available for the products listed in the FY 2005 FISMA Reporting Template?	*Yes*

The agency has implemented several policies that address security configurations and their implementation. In May 2003, the agency developed the NRC System Security Baseline Implementation Plan, with an objective to establish, develop, implement, maintain, and verify secure baseline configurations for all information systems. The NRC program is primarily based on the Center for Internet Security's benchmarks and scoring tools. NRC personnel compiled and researched recommended "best practice" technical settings and actions and developed "in house" benchmarks for those platforms for which a benchmark has yet to be developed. The following platforms were the focus of the initiative:

- Microsoft NT
- Microsoft Windows 2000
- Novell NetWare
- Sun Solaris
- IBM AIX
- Linux

The scope of the plan is all NRC systems running operating systems listed above and includes all systems that are currently in an "active" state and are components of the primary NRC network. Subsequent to the implementation of the System Security Baseline Implementation Plan, the agency has begun using the following additional benchmarks and configuration guides.

- Windows 2003 Domain Controllers and Member Servers (Center for Internet Security)
- Microsoft Internet Information Server (National Security Agency)

[9] NRC information systems are being re-certified and re-accredited in accordance with the minimum security controls for information systems defined in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems.*

- Microsoft SQL Server (National Security Agency)
- Router security configuration guide (National Security Agency)
- CISCO router Internet operating system (Center for Internet Security)
- CISCO PIX firewall (Center for Internet Security)
- HP-UX (Center for Internet Security)
- Apache (Center for Internet Security)
- Oracle (Center for Internet Security)

Oracle and Apache are currently not in production and are being tested for planned future production use. Hardening guidelines for Microsoft Internet Information Server are included with the Windows 2000/2003 configuration guides. The agency also uses Sybase, for which no specific configuration guides exist. However, the agency followed best practices and product guidelines from the vendor.

The Office of Information Services (OIS) has recently posted requirements on the NRC internal IT security Web page for the use of hardening specifications developed by the Center for Internet Security for all systems using Windows Server 2003 and Red Hat Linux. All deviations from the specification must be justified. Areas where the specification says: "if absolutely necessary" require justification of the "absolutely necessary" use of the feature. The same applies to the "disable if possible" areas (justify not disabling).

For desktops, NRC has developed a standard image for Windows XP that is based on NIST best practices. All desktops at NRC were upgraded to Windows XP in the past year. NRC uses workstation upgrades that are "pushed" at login to keep desktop configurations consistent across NRC. LANDesk can also be used to push upgrades to the desktops. NRC Announcements are used to announce agency workstation updates. The announcements describe the nature of the upgrade and that it will occur using an automated procedure that will occur during network login. The announcement includes, as an attachment, the schedule of when the upgrade will take place for each office in NRC.

NRC has also developed system security screening guidelines for preparing new systems for implementation into the NRC production operating environment. The security screening ensures that the system configuration meets NRC network security requirements. The guidelines outline the steps necessary to request and perform the security screening process, guidance on managing and developing a secure system, and industry best practices and additional resources.

3.9 Incident Detection and Handling Procedures

FY 2005 FISMA Reporting Template for Inspectors General Question 7

7.a. The agency follows documented policies and procedures for identifying and reporting incidents internally.	*Yes*

7.b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	*Yes*
7.c. The agency follows defined procedures for reporting to the United States Compnter Emergency Readiness Team (US-CERT).	*Yes*

NRC's Information Systems Security Incident Response Procedures (MD and Handbook 12.5 Appendix B) formalizes the agency's procedures for monitoring, detecting, reporting, and responding to information systems security incidents, and includes procedures for reporting incidents internally, for external reporting to law enforcement, and for reporting to the United States Computer Emergency Readiness Team (US-CERT).[10] The most current version of the incident response procedures are maintained on the agency's IT Web site.

The document defines the roles and responsibilities for reporting and responding to information systems security incidents. When criminal activity is suspected or confirmed, the procedures assign the OIG responsibility for contacting and coordinating the response with law enforcement officials.

3.10 Security Awareness and Training

FY 2005 FISMA Reporting Template for Inspectors General Questions 8, 9

8. Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?	*Mostly, or approximately 81-95% of employees have sufficient training*
9. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?	*Yes*

All new NRC employees (including contractors, interns, and summer hires) are required to attend orientation the first day they report for duty. During the orientation a brief presentation is made by a member of the OIS, Program Management, Policy Development, and Analysis Staff, Computer Security Team, which includes a discussion on appropriate use of information technology equipment. In addition, a member of the Office of the General Counsel also presents a section on ethics which includes additional discussions on appropriate use of the Internet.

All employees, including contractors, are required to take the on-line Computer Security Awareness course as soon as they receive a network UserID and every year thereafter. OIS maintains a database of personnel who have taken the security awareness course and cross checks the list on a regular basis with an employee list provided by NRC Human Resources. A member of the Computer Security Team sends a message to offices around the first of the month reminding them to have their employees take the course. Information System Security Officers must sign an acknowledgement of their responsibilities when taking the position and are required to take an on-line Information System Security Officer training course in addition to the on-line Computer Security Awareness course.

[10] The procedures actually reference reporting to the Federal Computer Incident Response Center, which was replaced with the US-CERT when the Department of Homeland Security was established.

NRC meets the Office of Personnel Management (OPM) requirement to expose employees to security awareness materials at least annually by (1) mandating all NRC staff take the NRC Computer Security Awareness course annually and by documenting who takes the annual training, (2) using posters, flyers, Web pages, NRC Yellow Announcements,[11] NRC Announcements,[12] and articles/notices in the NRC monthly newsletter to keep computer security on everyone's mind throughout the year, and (3) by holding the Annual NRC Computer Security Awareness Day event.

The agency is in the process of developing a computer security awareness and training program plan to fully implement the requirements outlined in OMB Circular A-130, *Management of Federal Resources*, Appendix III, *Security of Federal Automated Information Resources*, FISMA, MD and Handbook 12.5, and OPM's final regulations concerning information technology security awareness (5 CFR Part 930, Subpart C, effective June 14, 2004).

Agency staff and contractors are advised of the dangers of peer-to-peer applications during their annual Web-based security training. The on-line Computer Security Awareness course includes a discussion of the dangers of peer-to-peer applications such as instant messaging. Current agency policy does not explicitly prohibit peer-to-peer applications, however the agency is blocking sites that support the unauthorized reproduction of copyrighted material, i.e., peer-to-peer and file sharing Web sites.

Agency Lacks Procedures for Ensuring Employees With Significant IT Security Responsibilities Receive Security Training and Awareness

The agency stated that it had difficulty in gathering the information needed to report on the total number of employees with significant IT security responsibilities, the number of those employees who have received specialized training as described in NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, and the total costs for providing IT training. The agency's training system does not identify which employees have significant IT security responsibilities and what courses are considered related to IT security. The agency gathered its data by asking each office and region to identify staff in their offices with significant IT security responsibilities, describe any training that is related to IT security that those staff members have taken, and the cost of that training. The agency's training system also does not account for any training the employee may have taken on their own time.

[11] NRC Yellow Announcements (formerly Yellow Announcements) establish new policies, practices, or procedures; introduce changes in policy, senior staff assignments, or organization; or address major agencywide events. These announcements require signature and are retained as permanent records in ADAMS.

[12] NRC Announcements (formerly Network Announcements) communicate information of major significance or interest to agency employees, as well as urgent or time-sensitive information. These announcements do not require signature.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

10. Develop and implement procedures for ensuring employees and contractors with significant IT security responsibilities are identified, receive security awareness and training, and the individual and associated training are readily identifiable.

3.11 Agency Compliance with the Privacy Act

As part of the FY 2005 FISMA independent evaluation, the OIG asked Carson Associates to evaluate the agency's compliance with the Privacy Act. This request was made prior to OMB's issuance of the FY 2005 FISMA reporting guidelines, which also include a requirement to report on implementation of the Privacy Act. Carson Associates met with the agency's Privacy Program Officer and Web services representatives, and reviewed applicable agency policies, procedures, correspondence, and directives. Carson Associates used the questions found in the OMB Reporting Template for Senior Agency Officials for Privacy as guidance in performing the evaluation. Carson Associates found that controls for ensuring sufficient protections for privacy of personnel information as set forth in the E-Government Act are effective and that the agency is in compliance with the provisions of the Privacy Act.

[Page intentionally left blank]

4 Consolidated List of Recommendations

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Categorize all NRC information systems, including systems operated by a contractor or other organization on behalf of the agency, in accordance with FIPS 199.
2. Complete annual self-assessments for FY 2006 no later than August 1, 2006 and thereafter.
3. Develop and implement procedures to ensure contingency plans are tested annually, regardless of the status of the systems' certification and accreditation.
4. Maintain current copies of certification and accreditation memoranda for systems provided by other Federal agencies.
5. Maintain current copies of self-assessments for systems provided by other Federal agencies.
6. Maintain current copies of annual contingency plan testing results for systems provided by other Federal agencies.
7. Develop and implement procedures for performing oversight of major applications and general support systems operated by a contractor or other organization on behalf of the agency.
8. Review and update the six completed e-authentication risk assessments to correct inaccuracies and inconsistencies with FIPS 199 security categorizations.
9. Develop and implement a plan for completing the remaining e-authentication risk assessments.
10. Develop and implement procedures for ensuring employees and contractors with significant IT security responsibilities are identified, receive security awareness and training, and the individual and associated training are readily identifiable.

5 OIG Response to Agency Comments

OIG provided this report in draft to agency officials and discussed its content at an exit conference on September 22, 2005. We modified the report as we determined appropriate in response to our discussion. Agency officials generally agreed with the report's findings and recommendations and opted not to include formal comments.

SCOPE AND METHODOLOGY

The scope of this independent evaluation of NRC's Implementation of FISMA for FY 2005 included:

- NRC's AIS security program as described in MD an Handbook 12.5
- NRC's implementation of the Privacy Act

To conduct the independent evaluation, the independent evaluation team met with agency staff responsible for implementing the agency' AIS security program, reviewed certification and documentation for the agency's operational information systems, and reviewed other documentation provided by the agency that demonstrated their implementation of FISMA.

All analyses were performed in accordance with guidance from the following:

- National Institute of Standards and Technology standards and guidelines
- Nuclear Regulatory Commission Management Directive and Handbook 12.5, *NRC Automated Information Systems Security Program*
- NRC Office of the Inspector General audit guidance

This work was conducted between March 2005, and September 2005. The work was conducted by Jane M. Laroussi, CISSP; Diane Reilly; Kelby M. Funn, CISA; and S.J. Dobbs, CISA, from Richard S. Carson and Associates, Inc.

[Page intentionally left blank]

STATUS OF CONTINGENCY PLAN TESTING

The following information on the status of contingency plan testing was obtained from the 3rd Quarter FY 2005 POA&Ms submitted by the agency to OMB. This information is for the 24 operational systems that have not had their contingency plans tested in FY 2005.

System	Original Completion Date	Revised Completion Date	Comment
ADAMS	May 2005	August 31, 2005	Contingency plan test milestone included with weakness 05-2, complete security re-certification and re-accreditation for ADAMS.
Data Center	May 2005	July 2005	Contingency plan test milestone included with weakness 05-1, re-certify and re-accredit the NRC Data Center/Telecommunications System.
DDMS	June 1, 2004 (04-04) and April 1, 2005 (05-02)	August 1, 2005 (04-04 and 05-02)	Contingency plan testing included in weakness 04-04, complete contingency plan testing for DDMS, and 05-02, conduct annual testing of the system's contingency plan.
EHD	December 30, 2004 (04-04) and April 1, 2005 (05-2)	No new date specified, only that system has IATO through June 30, 2007 (04-04) and April 1, 2007 (05-2)	Contingency plan testing included in weakness 04-04, complete contingency plan testing for EHD, and 05-2, conduct annual testing of the system's contingency plan.
EIE	April 1, 2005 (05-2) and January 5, 2005 (05-6)	No new date specified, only that system has IATO through July 31, 2005 (05-2 and 05-7)	Contingency plan testing included in weakness 05-2, conduct annual testing of the system's contingency plan, and 05-7, approved contingency test and report.
ERDS	May 1, 2005 (05-2) and April 1, 2005 (05-3)	June 2, 2006 (05-3)	Contingency plan testing included in weakness 05-2, complete security re-certification and re-accreditation for ERDS, and 05-3, conduct the annual testing of the system's contingency plan.

System	Original Completion Date	Revised Completion Date	Comment
ETS	May 1, 2005 (05-2) and April 1, 2005 (05-3)	June 2, 2006 (05-3)	Contingency plan testing included in weakness 05-2, complete security re-certification and re-accreditation for ETS, and 05-3, conduct the annual testing of the system's contingency plan.
GLTS	May 2005 (05-2) and April 1, 2005 (05-3)	October 8, 2005 (05-2) and July 22, 2005 (05-3)	Contingency plan testing included in weakness 05-2, complete security re-certification and re-accreditation for GLTS, and 05-3, conduct the annual testing of the system's contingency plan.
HLW EHD			Not included in 3rd Quarter FY 2005 POA&M.
HPCS	March 10, 2005	No new date specified, only that system has IATO through December 31, 2005.	
IPSS	April 1, 2005	August 31, 2005	
LAN/WAN *	May 31, 2005	Not expected until FY06Q3	Contingency plan testing included in weakness 05-03, re-certify and re-accredit the NRC LAN/WAN.
LSN	July 31, 2005		Contingency plan testing included in weakness 05-2, complete security re-certification and re-accreditation for LSN.
LTS	July 2005		Contingency plan testing included in weakness 05-2, complete security re-certification and re-accreditation for LTS.
OCIMS	May 1, 2005 (05-2) and April 1, 2005 (05-3)	December 30, 2005 (05-2) and no new date specified, only that system has IATO through August 31, 2005 (05-3)	Contingency plan testing included in weakness 05-2, complete security re-certification and re-accreditation for ETS, and 05-3, conduct the annual testing of the system's contingency plan.

System	Original Completion Date	Revised Completion Date	Comment
RPS	November 12, 2004	Contingency plan test performed January 14, 2005 and report submitted to OIS.	Contingency plan testing included in weakness 05-2, complete security re-certification and re-accreditation for RPS. Carson Associates has not received documentation of the January 14, 2005 contingency plan testing described in the POA&M.
TAC	April 1, 2005 (05-2) and January 21, 2005 (05-8)	No new date, only note that system is to be transitioned to research and development role by December 31, 2005 and would no longer require certification and accreditation (05-2). 05-7 also includes note that system has IATO through June 30, 2005.	Contingency plan testing included in weakness 05-2, conduct the annual testing of the system's contingency plan, and 05-8, approved contingency test and report.

* The 3rd Quarter FY 2005 POA&Ms do not have a separate set of corrective actions for each of the eight general support systems resulting from the decomposition the old LAN/WAN.

[Page intentionally left blank]

Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name:

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2					
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
NRC	High	4	0	0	0	4	0	1	#DIV/0!	2	#DIV/0!	0	#DIV/0!
	Moderate	4	0	0	0	4	[illegible]	0	#DIV/0!	2	#DIV/0!	1	#DIV/0!
	Low	0	0	0	0	0	[illegible]	0	#DIV/0!		#DIV/0!	0	#DIV/0!
	Not Categorized	19	0	7	0	26	[illegible]	10	#DIV/0!	17	#DIV/0!	5	#DIV/0!
	Sub-total	**27**	**0**	**7**	**0**	**34**	[illegible]	**11**	**#DIV/0!**	**21**	**#DIV/0!**	**6**	**#DIV/0!**
Bureau	High					0	[illegible]		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					[illegible]	[illegible]		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Agency Totals	**High**	**4**	**0**	**0**	**0**	**4**	**0**	**1**	#DIV/0!	**2**	#DIV/0!	**0**	#DIV/0!
	Moderate	**4**	**0**	**0**	**0**	**4**	**0**	**0**	#DIV/0!	**2**	#DIV/0!	**1**	#DIV/0!
	Low	**0**	**0**	**0**	**0**	**0**	**0**	**0**	#DIV/0!	**0**	#DIV/0!	**0**	#DIV/0!
	Not Categorized	**19**	**0**	**7**	**0**	**26**	**0**	**10**	#DIV/0!	**17**	#DIV/0!	**5**	#DIV/0!
	Total	**27**	**0**	**7**	**0**	**34**	**0**	**11**	#DIV/0!	**21**	#DIV/0!	**6**	#DIV/0!

Question 3		
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory		
3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient Response Categories: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time	- Mostly, for example, approximately 81-95% of the time
3.b.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency Response Categories: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 51-70% complete
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	no
3.d.	The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	no
3.f.	The agency has completed system e-authentication risk assessments.	Yes
Question 4		
Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below. For items 4a.-4.f, the response categories are as follows: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time		
4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	- Almost Always, for example, approximately 96-100% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	- Almost Always, for example, approximately 96-100% of the time
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% of the time
4.e.	OIG findings are incorporated into the POA&M process.	- Almost Always, for example, approximately 96-100% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Almost Always, for example, approximately 96-100% of the time
Comments: NRC has two primary tools for tracking IT security weaknesses. At a high level, NRC uses the POA&M submitted to OMB to track corrective actions from the OIG annual independent evaluation, and the agency's annual review. The POA&M may also include corrective actions resulting from other security studies conducted by or on behalf of NRC. At a more detailed level, NRC uses an internal system to track the progress of more specific corrective actions, such as those resulting from risk assessments, security test and evaluation associated with the certification and accreditation process, and contingency plan testing.		

Question 5	
OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assesament of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initialed after May, 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans .	
Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Poor
Comments: See attached narrative.	

Section B: Inspector General. Question 6, 7, 8, and 9.

Agency Name:

Question 6

6.a.	Is there an agency wide security configuration policy? Yes or No.	Yes
	Comments:	

6.b. Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	Addressed in agencywide policy? Yes, No, or N/A.	Do any agency systems run this software? Yes or No.	Approximate the extent of implementation of the security configuration policy on the systems running the software. Response choices include: - Rarely, or, on approximately 0-50% of the systems running this software - Sometimes, or on approximately 51-70% of the systems running this software - Frequently, or on approximately 71-80% of the systems running this software - Mostly, or on approximately 81-95% of the systems running this software - Almost Always, or on approximately 96-100% of the systems running this software
Windows XP Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Professional	N/A	No	
Windows 2000 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2003 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Solaris	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
HP-UX	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Linux	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Cisco Router IOS	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Oracle	N/A	No	
Other. Specify: Novell, AIX, Sybase, SQL Server, Cisco PIX, IIS, Apache	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software

Comments: Oracle and Apache - configuration guides are available, but this software is currently not in production. Oracle and Apache are being tested for planned future production use. IIS - hardening guidelines are included in the Windows 2000/2003 configuration guides. Sybase - no specific configuration guides exist, however the agency followed best practices and product guidelines from the vendor.

Question 7

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes

Comments:

	Question 8	
8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training
	Question 9	
9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes

The following supplemental information is provided in support of the Office of Management and Budget FY 2005 Federal Information Security Management Act (FISMA) Reporting Template for Agency Inspectors General for the Nuclear Regulatory Commission (NRC). The independent evaluation of NRC's implementation of FISMA for FY 2005 was conducted by Richard S. Carson and Associates, Inc. (Carson Associates) on the behalf of the NRC Office of the Inspector General (OIG).

Question 1a. NRC has a total of 30 production systems. Of the 30, 12 are general support systems (all operational), and 18 are major applications (15 operational, 3 in development). As required by FISMA, the OIG selected five NRC operational systems for evaluation during the FY 2005 FISMA independent evaluation. However, during a status meeting with the agency, the OIG learned that the certification and accreditations of the systems chosen for evaluation had either expired and the systems were operating under an interim authorization to operate (IATO), or were due to expire in FY 2005, and that their re-certification and re-accreditation would not be completed before completion of the FY 2005 FISMA independent evaluation. Furthermore, there were no other systems to substitute because they were either reviewed during the FY 2004 FISMA independent evaluation, or had certification and accreditations that were due to expire before the end of the year. Without enough systems with current certification and accreditations, Carson Associates could not perform an evaluation of a representative subset of agency systems for the FY 2005 FISMA independent evaluation.

Question 1b. NRC has a total of seven systems operated by a contractor or other organization on behalf of the agency (two major applications and five general support systems). Of the seven, three are operated by other Federal agencies, two are operated by federally funded research and development centers, and two are operated by contractors supporting the agency. Carson Associates did not review any of the seven systems operated by a contractor or other organization on behalf of the agency for evaluation during the FY 2005 FISMA independent evaluation, as there were no potential candidates to review. Of the seven, four[13] were evaluated

[13] The FY 2004 FISMA independent evaluation included a review of three contractor operations and facilities. These three contractor operations and facilities support a total of four agency systems operated by a contractor or other organization on the behalf of the agency.

during the FY 2004 FISMA independent evaluation (three operated by other Federal agencies and one operated by a federally funded research and development center), and therefore were not candidates for review in FY 2005. The other three systems operated by a contractor or other organization on behalf of the agency were not candidates for evaluation in FY 2005 because there was not sufficient information available to perform an evaluation. The agency stated that in FY 2005 it would be performing self-assessments in accordance with NIST SP 800-26 on its contractor systems. However, the self-assessments were not completed in time for inclusion in the FY 2005 FISMA independent evaluation.

Question 2. Since Carson Associates was unable to evaluate any of NRC's systems, the metrics in Question 2 represent the status for all NRC systems, not just a subset of systems.

Question 2a. Of the 11 systems that are certified and accredited, 3 are systems operated by a contractor or other organization on behalf of the agency. These three systems are operated by other Federal agencies. NRC presumes that the two Federal agencies that operate these systems are also following FISMA and guidelines from the National Institute of Standards and Technology (NIST) (these agencies have not allowed NRC to conduct their own review). Carson Associates verified that there are agreements in place with the two Federal agencies providing services to NRC and that the agreements include requirements to comply with applicable Federal and respective agency information systems security policies, mandates, and instructions. However, the agency does not maintain copies of all certification and accreditation documentation for these systems. The other four systems operated by a contractor or other organization on behalf of the agency have not been certified and accredited.

Question 2b. NRC meets the FISMA requirement to test and evaluate the security controls of agency information system by performing annual self-assessments on the systems. NRC developed self-assessment templates for major applications and general support systems. For FY 2005 NRC also developed a site self-assessment template for security assessments at regional offices, resident inspector sites, NRC locations other than headquarters and the regional offices, and contractor sites hosting NRC information systems. The NRC self-assessment templates are based on NIST SP 800-26 and include references to NIST SP 800-53 to provide a general indication of control coverage. However, as of September 12, 2005, Carson Associates had only received self-assessments for 18 of the NRC's 27 operational systems.[14] The first self-assessment was not received until September 2, 2005. Subsequent to completion of field work, the agency provided self-assessments for the other nine operational systems. However, these self-assessments were not provided in time to review.

Of the 21 systems that have had their security controls tested and evaluated in the last year, 3 are systems operated by a contractor or other organization on behalf of the agency. These three systems are operated by other Federal agencies. NRC presumes that the two Federal agencies that operate these systems are also following FISMA and NIST guidelines (these agencies have not allowed NRC to conduct their own review), and have therefore conducted an annual review. However, the agency does not request a copy of the annual review for these systems from the other Federal agencies. As previously discussed, the agency stated that in FY 2005 it would be performing self-assessments on its contractor systems. However, Carson Associates has not

[14] One of the self-assessments addresses eight individual general support systems.

received any self-assessments for the four other systems operated by a contractor or other organization on behalf of the agency. Subsequent to completion of field work, the agency provided self-assessments for the four other systems operated by a contractor or other organization on behalf of the agency. However, these self-assessments were not provided in time to review.

Question 2c. Of the 6 systems that have had their contingency plans tested in the last year, 3 are systems operated by a contractor or other organization on behalf of the agency. These three systems are operated by other Federal agencies. NRC presumes that the two Federal agencies that operate these systems are also following FISMA and NIST guidelines (these agencies have not allowed NRC to conduct their own review), and have therefore performed an annual contingency plan test of their systems. However, the agency does not verify that the contingency plans have been tested and evaluated for these systems on an annual basis. The agency does not have contingency plans for the other four systems operated by a contractor or other organization on behalf of the agency. Subsequent to the completion of field work, Carson Associates was informed that contingency plan testing had been performed on 10 additional agency systems (8 of which are general support systems resulting from the decomposition of the agency's local area network/wide area network general support system). However, the agency has not provided documentation indicating the testing has been completed.

Question 3a. As previously discussed, NRC presumes that the two Federal agencies that operate three of the seven contractor systems are also following FISMA and NIST guidelines (these agencies have not allowed NRC to conduct their own review). However, the agency does not (1) maintain copies of all certification and accreditation documentation for these systems, (2) verify that the security controls have been tested and evaluated for these systems on an annual basis, and (3) verify that the contingency plans have been tested and evaluated for these systems on an annual basis.

The agency has not performed sufficient oversight and evaluation of four of the seven contractor systems to ensure the information systems meet requirements of FISMA, OMB policy, NIST guidelines, and agency policy. The agency stated that for two of the four systems (the two contractor support systems), security guidelines are written into the relevant contracts and the contractors must follow NRC security procedures. However, the agency has no documentation demonstrating that these systems meet FISMA requirements, specifically the requirement for certification and accreditation, annual testing and evaluation of security controls, and annual contingency plan testing. Carson Associates could not determine how NRC performs oversight of the other two contractor systems (the two federally funded research and development centers).

Question 3b. NRC maintains information on its information systems in two different inventory systems. One is primarily used to meet the requirements of FISMA, while the other is primarily used to support the agency's enterprise architecture. While FISMA only requires agencies to maintain an inventory of major information systems (major applications and general support systems), NRC also includes two other types of systems in its inventories – Listed[15] and Other.[16] Carson Associates found that the agency's inventory is only 51-70 percent completed because (1) information in both of the agency's inventory systems is inaccurate and inconsistent and (2) only one of the inventory systems contains information on system interfaces and that information is also inaccurate and inconsistent.

Question 3.c. Carson Associates generally agrees with the Chief Information Officer (CIO) on the number of agency owned major applications and general support systems, but does not agree with the CIO on the number of agency owned systems in the listed and other categories.

Question 3f. In FY 2004, the agency stated that it had begun assessing systems for e-authentication risk. A contract was awarded in the 3rd Quarter FY 2004 and the agency stated it was on track to meet the December 15, 2004, deadline for classifying all major applications. However, Carson Associates found that e-authentication risk assessments have been completed for only 6 of the agency's 27 operational systems. The agency stated that e-authentication risk assessments will be supported under the interim Information Systems Security contract awarded August 11, 2005 and are expected to be completed by December 15, 2005. Carson Associates reviewed the completed e-authentication risk assessments and round them to be incorrect and inconsistent with the systems' FIPS 199 security categorizations.

Question 5. As stated previously, only 8 of the 27 operational NRC information systems have full authorization to operate (i.e., they have a current certification and accreditation). As a result, the NRC Office of the Inspector General requested Carson Associates to undertake an overall review of the NRC's certification and accreditation efforts. The findings from this review were reported in a separate report that made two recommendations to the agency to improve certification and accreditation efforts at the agency. The following is a summary of the findings from the evaluation of NRC's certification and accreditation efforts.

NRC's general support systems have not had a full certification and accreditation performed in the past 3 years. Therefore the agency does not know whether the security controls for these general support systems are adequate, creating unknown potential risk. As a result, all NRC information systems that depend on the security controls provided by these general support systems inherit that unknown potential risk. The majority of NRC information systems are not certified and accredited because (1) the certification and accreditation has lapsed or was never completed and (2) NRC information systems are being re-certified and re-accredited using new NIST requirements. As a result, potential risks to agency information systems are unknown.

[15] A Listed system is a computerized information system or application that (1) processes sensitive information requiring additional security protections and (2) may be important to an NRC office's or region's operations, but which is not a major application or general support system when viewed from an agency perspective. Sensitive data may include individual Privacy Act information, law enforcement sensitive information, sensitive contractual and financial information, safeguards, and classified information.

[16] An Other system is an NRC system that does not require additional security protections and is adequately protected by the security provided by the NRC local area network/wide area network.

Question 8. NRC ensures all employees and contractors receive security awareness and training. However, the agency lacks procedures for ensuring employees with significant information technology (IT) security responsibilities receive security training and awareness. The agency stated that it had difficulty in gathering the information needed to report on the total number of employees with significant IT security responsibilities, the number of those employees who have received specialized training as described in NIST SP 800-16, and the total costs for providing IT training. The agency's training system does not identify which employees have significant IT security responsibilities and what courses are considered related to IT security. The agency gathered its data by asking each office and region to identify staff in their offices with significant IT security responsibilities, describe any training that is related to IT security that those staff members have taken, and the cost of that training. The agency's training system also does not account for any training the employee may have taken on their own time.